(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－242470
（P2000－242470A）
(43)公開日　平成12年９月８日(2000.9.8)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ	7/58	Ａ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｂ	
Ｈ０４Ｌ	9/24		Ｈ０４Ｌ	9/00	６５７	

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平11－44365

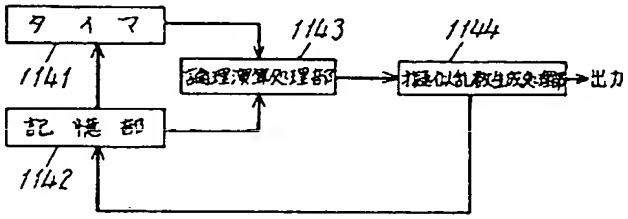
(22)出願日　平成11年２月23日(1999.2.23)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　樋口　淑夫
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5J104 FA00 GA03 GA04 NA04 NA35

(54)【発明の名称】　乱数生成装置および方法および記録媒体

(57)【要約】
【課題】　乱数生成の際に必要なシード値を装置内部で自動的に生成し、外部からの解析にも強固な乱数を生成する。
【解決手段】　装置の起動時、タイマ１１４１に記憶部１１４２からデータを転送し、タイマ１１４１の計数を開始する。乱数生成時、タイマ１１４１の計数値と記憶部１１４２のデータを用いて論理演算処理部１１４３で論理演算を行い、演算結果を初期シード値として、擬似乱数生成処理部１１４４の初期値として入力することにより出力に乱数が得られる。生成した乱数の一部を記憶部１１４２にフィードバックする。



1

【特許請求の範囲】
【請求項１】タイマの値と記憶部が格納するデータ値からシード値を生成する論理演算処理部と、
前記シード値から乱数を生成する擬似乱数生成処理部と、を備えることを特徴とする乱数生成装置。
【請求項２】前記記憶部は、
生成した乱数をフィードバックして保持することを特徴とする請求項１記載の乱数生成装置。
【請求項３】前記タイマは、
動作開始時に前記記憶部が格納するデータ値を開始点として計数することを特徴とする請求項１記載の乱数生成装置。
【請求項４】記憶部からデータを取得し、取得したデータをタイマの開始点として計数を行う計数処理手段と、
記憶部からデータを取得し、前記タイマと前記取得データからシード値を生成する論理演算処理手段と、
前記シード値から乱数を生成する擬似乱数生成処理手段と、
前記乱数を前記記憶部にフィードバックして記録する記録処理手段と、を備えることを特徴とする乱数生成方法。
【請求項５】記憶部からデータを取得し、取得したデータをタイマの開始点として計数を行う計数処理手段と、
前記記憶部からデータを取得し、前記タイマと前記取得データからシード値を生成する論理演算処理手段と、
前記シード値から乱数を生成する擬似乱数生成処理手段と、
前記乱数を前記記憶部にフィードバックして記録する記録処理手段と、を備えることを特徴とする乱数生成プログラムを格納した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、自分自身で電源を持たない回路および装置上で、自動的に乱数を生成する乱数生成装置および方法および記録媒体に関するものである。
【０００２】
【従来の技術】近年、情報通信システムの発展とともに、データ通信の安全性を高めるセキュリティ技術の重要性が高まっている。なかでも、乱数生成技術は安全なデータ通信を保証するために利用する暗号化技術には不可欠なものであり、主な用途として、ワンタイムパスワードの作成、暗号化に使用する鍵値の作成、暗号文の生成、電子署名情報の生成等がある。
【０００３】暗号化技術を利用すれば、データの暗号化、および、本人認証に必要な電子署名の生成を行うことができる。これらの技術は、処理性能の高いパーソナルコンピュータやワークステーションなどのデスクトップコンピュータ上で行われてきていたが、電子マネーやＩＤカードによる個人用途向けのセキュリティシステム

2

等で利用するために、ＩＣカード上に実装したマイクロコンピュータにおいて乱数を生成し、暗号化技術を利用する必要性が生じている。
【０００４】従来より、回路および装置を用いて乱数の生成を行う場合には、物理手段を利用して乱数列を発生させる方式と数学的な演算処理を行い、長周期の乱数列を生成する擬似乱数生成方式の２種類の方式を用いている。さらに、通信のセキュリティを確保するための暗号化技術においても、このようにして生成された乱数が用いられているが、電子マネーやＩＤカード等の個人向けのセキュリティ用途で使用する場合には、乱数生成方式の実用性と生成した乱数の安全性が特に重要になってくる。
【０００５】物理手段を利用して乱数列を発生させる多数の方式が知られている。以下、物理手段を利用して乱数を発生させる方式について述べる。この例としては、抵抗体の熱雑音により乱数を生成する方式があげられる。抵抗体の熱雑音は多数の電子により発生する微少電流を合成したものであり、それぞれの電子の衝突・散乱は無関係に発生するため、雑音は一様に発生する。高抵抗の両端に発生する微少な雑音電圧を、ハイインピーダンス・低雑音のアンプで増幅して雑音電圧を取得し、その電圧をＡ／Ｄコンバータでデジタルデータに変換してパーソナルコンピュータやワークステーションに入力、棄却法やくくり合わせ法などの処理を行うことによって、乱数の性質の改善を行うことができ、適切な乱数が得られる。
【０００６】この方式は、物理的な性質を利用するので、０と１の発生確率がおのおの約１／２になり、各ビットが他の部分と独立であるので、生成される乱数列の推測は困難であり、セキュリティの用途に適した乱数列が得られるが、特別なハードウェアを必要とするので非常にコストがかかり、特に、マイクロコンピュータ上に実装しての利用には不向きである。
【０００７】擬似乱数生成方式として多数の方式が知られている。以下、擬似乱数生成方式により乱数を生成する方式について述べる。この例としては、線形フィードバックシフトレジスタによる方式があげられる。図８は線形フィードバックシフトレジスタの例であり、２０１はシフトレジスタのセル、２０２は排他的論理和回路、２０３はシフトレジスタの出力である。出力される乱数列は、シフトレジスタ２０１の個数、排他的論理和回路２０２の構成によって異なり、図８に示す構成に限られるものではない。
【０００８】以上のように構成された線形フィードバックシフトレジスタについて、以下、その動作を説明する。最初に、シフトレジスタのセル２０１にそれぞれ初期値を設定し、シフトレジスタのセル２０１の内容から排他的論理和回路２０２により論理演算を行い、演算結果をシフトレジスタの出力２０３に出力する。１ビット

を出力するごとに、シフトレジスタのセル２０１のデータを矢印の方向にシフトさせていき、出力はシフトレジスタのセル２０１にフィードバックしてシフトを繰り返していく。この結果、ｎ段を有するシフトレジスタは最大$N=2^{n-1}$ビット長の非周期的ビット列を生成し得ることになり、段数の多いシフトレジスタを使用すれば、長周期の擬似乱数が得られる。

【０００９】この装置は、特別なハードウェアを必要とせず、ソフトウェアによる実現が可能であり、マイクロコンピュータ上で利用できるが、シフトレジスタのセル２０１の初期値により乱数列が生成されるためにシフトレジスタの構成およびシフトレジスタの初期値が判明すれば同様の乱数列を容易に生成し得ることが欠点である。擬似乱数生成方式として他に線形合同法、暗号技術による方法、デジタルカオス法等があげられるが、これらも同様の欠点を持っている。

【００１０】したがって、擬似乱数生成方式を利用して乱数を生成するには、乱数を生成するごとに初期シード値を設定する必要がある。一般的に、パーソナルコンピュータやワークステーション上では初期シード値として、システムが保有している現在時刻が用いられている。

【００１１】

【発明が解決しようとする課題】しかしながら、非接触型のＩＣカードのような内部で現在時刻などのリアルタイムに変化するデータを持っていないシステムでは、外部から初期シード値を供給する必要がある。図９は外部から初期シード値を供給して乱数を生成する一実施の形態であり、２１１はマイクロコンピュータ、２１２はマイクロコンピュータ２１１の外部入力、２１３はマイクロコンピュータ２１１に実装した擬似乱数生成処理部、２１４はマイクロコンピュータ２１１の外部出力である。まず、外部入力２１２から入力された初期シード値は、擬似乱数生成処理部２１３で初期シード値に設定されて乱数を生成し、外部出力２１４に乱数を出力する。

【００１２】図９のような上記従来の構成では、外部入力２１２から初期シード値を盗聴することが可能であり、入出力の相関関係から内部の擬似乱数生成処理部が解析できるため、安全であるとはいい難い。

【００１３】本発明は、上記従来の問題点を解決するもので、自分自身で電源を持たない装置上で、外部からの入力により初期シード値を設定することなく、自身で閉じて乱数を生成する乱数生成装置および方法および記録媒体を提供することを目的とする。

【００１４】

【課題を解決するための手段】上述課題を解決するために、請求項１にかかる発明は、タイマの値と記憶部が格納するデータ値からシード値を生成する論理演算処理部と前記シード値から乱数を生成する擬似乱数生成処理部を備えることを特徴とする乱数生成装置としている。

【００１５】また、請求項２にかかる発明においては、前記記憶部は、生成した乱数をフィードバックして保持することを特徴とする請求項１記載の乱数生成装置としている。

【００１６】さらに、請求項３にかかる発明においては、前記タイマは、動作開始時に前記記憶部が格納するデータ値を開始点として計数することを特徴とする請求項１記載の乱数生成装置としている。

【００１７】前記構成によって、起動時ごとに異なるタイマの値と記憶部に蓄積されているデータから、擬似乱数生成の際に用いる初期シード値を自動的に生成することができるので、自分自身で電源を持たない回路および装置上でも安全性の高い乱数を低コストで生成することができる。

【００１８】

【発明の実施の形態】以下、本発明の一実施の形態として、乱数生成装置について説明する。なお、本実施の形態では装置による実施の形態について説明しているが、本発明は装置に限定するものではなく、ソフトウェアにより機能を実現してもよい。

（１）乱数生成装置を用いたシステム

図１は、本実施形態における乱数生成装置を用いたシステム例として、ＩＣカード内蔵マイクロコンピュータを用いた暗号処理システムについて説明している。図１において、１０はＩＣカード、１１はＩＣカード１０に内蔵されている自身で電源を内蔵していないマイクロコンピュータ、１２はＩＣカード１０とのデータの通信を行う通信機、１３は通信機１２の制御を行う制御機器である。まず、図１のＩＣカード１０の存在を確認後、制御機器１３から通信機１２に指示を与え、ＩＣカード１０に通信機１２から電力を供給する。マイクロコンピュータ１１は自身で電源を持たないので、通信機１２から電力の供給を受けて起動、動作を行う。一方、マイクロコンピュータ１１を起動後、制御機器１３から、通信機１２を経由して、データを伝送し、マイクロコンピュータ１１において乱数を生成し、生成した乱数を利用してマイクロコンピュータ１１内部で暗号処理を行う。暗号処理後のデータは、通信機器１２を経由して、制御機器１３に伝送される。

【００１９】図２は、マイクロコンピュータ１１の処理の構成をあらわすブロック図である。図２において、１１１はＩＣカード１０に送受信されるデータの処理を行うＩ／Ｏ処理部、１１２はマイクロコンピュータ１１における処理全般の制御を行うＯＳ処理部、１１３はデータの暗号化を行う暗号処理部、１１４は暗号化を行う際に用いる乱数を生成する乱数生成部である。ＩＣカード１０に送信されたデータはマイクロコンピュータ11で処理される。マイクロコンピュータ１１においてデータは、Ｉ／Ｏ処理部１１１、ＯＳ処理部１１２で処理が行われ、暗号処理部１１３に渡される。一方、乱数生成部

5

１１４では、暗号処理部１１３から乱数の要求があった際に乱数を生成し、暗号処理部１１３に送る。暗号処理部１１３では、前記入力データを前記乱数で暗号化し、暗号化されたデータはＯＳ処理部１１２を経由して、Ｉ／Ｏ処理部１１Ｉに渡し、通信機１２へと伝送する。

【００２０】なお、本乱数生成装置は、前記実施形態に限定するものではなく、乱数の生成を必要とする電子署名生成システムにも利用できる。電子署名を生成するには、図２において、暗号処理部で行っている処理の代わりに電子署名の生成を行えばよい。

（２）乱数生成装置の詳細

上記のように乱数は乱数生成部１１４で生成される。ここでは、図３は乱数生成部１１４の構成をあらわすブロック図を参照して説明を行う。図３において、１１４１はマイクロコンピュータ１１の動作開始時点から乱数生成部１１４における乱数の生成開始時点までの時間を計測するタイマ、１１４２は生成した乱数をフィードバックして蓄積する記憶部、１１４３は乱数の初期シード値を生成する論理演算処理部、１１４４は初期シード値から擬似乱数を生成する擬似乱数生成処理部である。まず、タイマ１１４１はマイクロコンピュータ１１に通信機１２から電力が供給され起動した際に、記憶部１１４２からタイマにデータを転送し、カウンタの開始時点とする。次に、タイマ１１４１の計数を開始し、論理演算処理部１１４３での処理を開始するまで計数を継続する。なお、初回の乱数生成時には、記憶部１１４２にあらかじめ装置のシリアル番号等のデータを蓄積しておくとよい。乱数を生成する際には、前記タイマが計数している値と記憶部１１４２に蓄積されているデータを論理演算処理部１１４３において論理演算を行い、演算結果を初期シード値として擬似乱数生成処理部１１４４に入力して乱数を生成する。生成された乱数の一部または全てのデータを記憶部１１４２にフィードバックして以前に蓄積していたデータに上書きし、次回の乱数生成時に利用する。なお、論理演算処理部１１４３、擬似乱数生成処理部１１４４における処理はハードウェア、ソフトウェアのどちらで機能を実現してもよい。

【００２１】以下、図４のフローチャートを参照して、本実施の形態における乱数生成処理の概略について説明する。

(ステップＳ３０１)マイクロコンピュータ１１の起動時、記憶部１１４２からデータを取得し、タイマ１１４１に転送する。その値から計数を開始し、論理演算処理部１１４３における論理演算の開始時まで計数を継続する。ステップＳ３０２に行く。

(ステップＳ３０２)論理演算処理部１１４３においてタイマ１１４１の計数値と記憶部１１４２のデータを取得し、これら２値の論理演算を行う。乱数の初期シード値を生成する。ステップＳ３０３に行く。

(ステップＳ３０３)前記初期シード値を擬似乱数生成処理部１１４４に入力して乱数を得る。ステップＳ３０４に行く。

6

(ステップＳ３０４)前記乱数をフィードバックして記憶部１１４２に蓄積する。以下、図５のフローチャートを参照して、本実施の形態における乱数生成装置の動作の詳細について説明する。

(ステップＳ４０１)制御機器１３からの指示を通信機１２が受信し、通信機１２とデータの送受信を行うＩＣカード１０が存在することを確認する。存在すれば、ステップＳ４０２に行く。存在しなければ、ステップＳ４０１に戻る。

(ステップＳ４０２)通信機１２からＩＣカード１０に電力を供給する。ステップＳ４０３に行く。

(ステップＳ４０３)ＩＣカード１０は通信機１２から供給された電力により、マイクロコンピュータ１１を起動する。同時に、記憶部１１４２からタイマ１１４１にデータを転送し、タイマ１１４１は計数を開始する。ステップＳ４０４に行く。

(ステップＳ４０４)制御機器１３から指示に基づき、通信機１２を介在して、暗号化するデータをＩＣカード１０に伝送する。ステップＳ４０５に行く。

(ステップＳ４０５)ＩＣカード１０がデータを受信すれば、ステップＳ４０６に行く。受信できていなければ、ステップＳ４０４に戻る。

(ステップＳ４０６)暗号化を開始する指示を乱数生成部１１４に出す。ステップＳ４０７に行く。

(ステップＳ４０７)暗号化開始の要求を受け、起動していたタイマ１１４１を停止する。ステップＳ４０８に行く。

(ステップＳ４０８)タイマ１１４１と記憶部１１４２の値に対して、論理演算処理部１１４３で論理演算を行い、初期シード値を生成する。ステップＳ４０９に行く。

(ステップＳ４０９)初期シード値を擬似乱数生成処理部１１４４に入力し、乱数を得る。得た乱数は記憶部１１４２に蓄積しておく。ステップＳ４１０に行く。

(ステップＳ４１０)生成した乱数および受信したデータを暗号処理部１１３に入力、暗号化を行い、暗号化データを得る。ステップＳ４１１に行く。

(ステップＳ４１１)通信機１２を介在して、暗号化データをＩＣカード１０から制御機器１３に伝送する。通信機１２はＩＣカードへの電力の供給を終了する。ステップＳ４０１に戻る。

【００２２】以上のように本実施形態によれば、論理演算処理部１１４３での演算処理を行うまでには、ＩＣカード１０と通信機１２との間の通信処理時間、ＯＳ処理部１１２での処理時間が含まれ、これらの処理時間は処理するデータおよびシステムを実施する環境によって異なる。すなわち、乱数を生成するごとにタイマ１１４１による計数値は異なる計数値となる。さらに、タイマ１

7

１４１によって計数された値のみでは、値のバラツキが小さくなる可能性があるので、タイマ１１４１における計数の開始時点の値を記憶部１１４２のデータから取得するとともに、記憶部１１４２のデータとの論理演算を行うことによって値のバラツキの範囲を広範囲かつ予測不可能にしている。

【００２３】外部からの解析によって、擬似乱数生成処理部１１４４による擬似乱数生成方式および記憶部１１４２に蓄えられているデータが判明した場合、生成される乱数が予測される可能性がある。しかし、上記で説明したようにタイマ１１４１のカウンタの値は通信環境により毎回異なるので、タイマ１１４１の値と記憶部１１４２に蓄えられているデータの２値を用いて論理演算を行った値を正確に予測することは困難であり、この値が１ビットでも異なれば、擬似乱数生成処理部１１４４はまったく異なった乱数を生成するので、外部からの解析にも強固な乱数生成装置となる。

【００２４】なお、擬似乱数生成処理部１１４４で利用する方式としては線形フィードバックシフトレジスタがあげられる。他にも線形合同法、暗号技術による方法、デジタルカオス法等の初期シード値を必要とする擬似乱数生成方式により行ってもよい。

（３）演算処理部の詳細

上記のように論理演算処理部１１４３では擬似乱数生成処理部１１４４への初期シード値を生成するために論理演算を行う。ここでは、図６を参照して論理演算処理部１１４３の具体的な一実施形態について説明する。図６において、１１４１はタイマであり、１１４２は記憶部であり、１１４５は排他的論理和回路、１１４６は論理演算処理部１１４３の出力である。まず、タイマ１１４１の値は上位ビット列と下位ビット列に分割してビット列の上位部分と下位部分の位置を反転する。一方、記憶部１１４２に蓄積されているデータも上位ビット列と下位ビット列に分割し、上記の反転した値とそれぞれ排他的論理和の演算を行う。次に、それぞれのビット列を再び結合して論理演算処理部１１４３の出力１１４６とし、この出力値を初期シード値として擬似乱数生成処理部１１４４に入力し乱数を得る。

【００２５】最大周期が長いタイマを利用した際には、マイクロコンピュータ１１の起動時から乱数生成時までの時間が極端に短い場合、タイマ１１４１の上位ビットが開始時点から変化がないこともありえるが、タイマ１１４１の値の上位ビット列と下位ビット列を反転することにより、最大周期が長いタイマを利用したとしても、排他的論理和の演算を行った際に出力１１４６の上位ビットが全て０になることはない。なお、論理演算処理部１１４３は上記の方式に限定するものではない。

（４）記憶部内のデータ

本実施形態における記憶部１１４２内の記録方式の一実施形態を図７に示す　実施形態としては、記憶部１１４２内の特定のアドレスを指定しておき、そのアドレスを開始点としてデータを蓄積すればよい。乱数生成を行うごとに同じアドレスに上書きして前回のデータを残さないようにしておくようにする。上記のように記憶することにより、暗号化の際に利用した乱数データが判明しないようにしておく。

【００２６】

【発明の効果】本発明は、タイマと擬似乱数生成処理部からデータのフィードバックを行う記憶部を利用することにより、特別なハードウェアを追加することなく、装置内部で自動的に乱数を生成できる優れた乱数生成装置および方法および記録媒体を実現するものである。

【図面の簡単な説明】

【図１】ＩＣカードを用いた暗号処理システムの構成図

【図２】ＩＣカード内蔵マイクロコンピュータのブロック構成図

【図３】本発明の一実施形態における構成図

【図４】本発明の乱数生成処理のフローチャート

【図５】本発明の一実施形態におけるフローチャート

【図６】本発明の一実施形態における演算処理部の構成図

【図７】記憶部内のデータに関する概略図

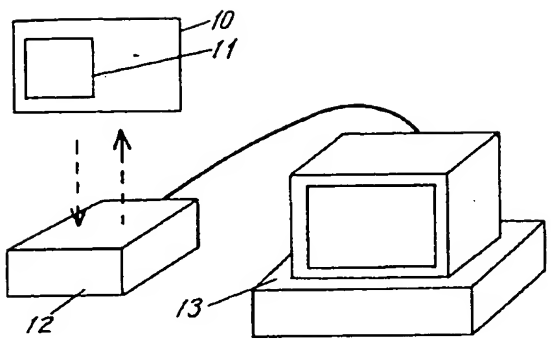
【図８】数学的な演算処理により擬似乱数列を生成する従来例の回路図

【図９】擬似乱数生成処理部を利用して乱数を生成する従来例の構成図

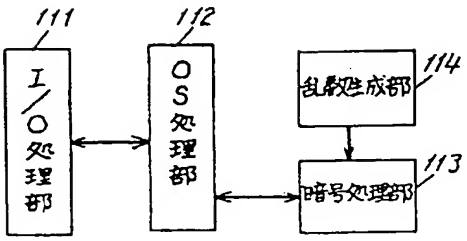
【符号の説明】

１０　ＩＣカード
１１　マイクロコンピュータ
１２　通信機
１３　制御機器
１１１　Ｉ／Ｏ処理部
１１２　ＯＳ処理部
１１３　暗号処理部
１１４　乱数生成部
２０１　シフトレジスタのセル
２０２　排他的論理和回路
２０３　シフトレジスタの出力
２１１　マイクロコンピュータ
２１２　マイクロコンピュータの外部入力
２１３　擬似乱数生成処理部
２１４　マイクロコンピュータの外部出力
１１４１　タイマ
１１４２　記憶部
１１４３　論理演算処理部
１１４４　擬似乱数生成処理部
１１４５　排他的論理和回路
１１４６　論理演算処理部出力

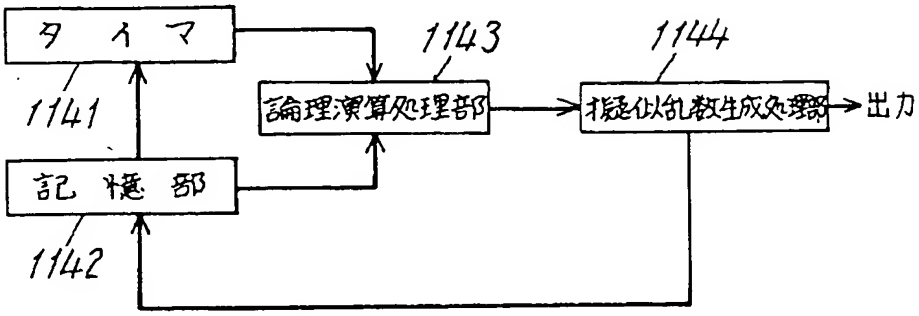
【図１】



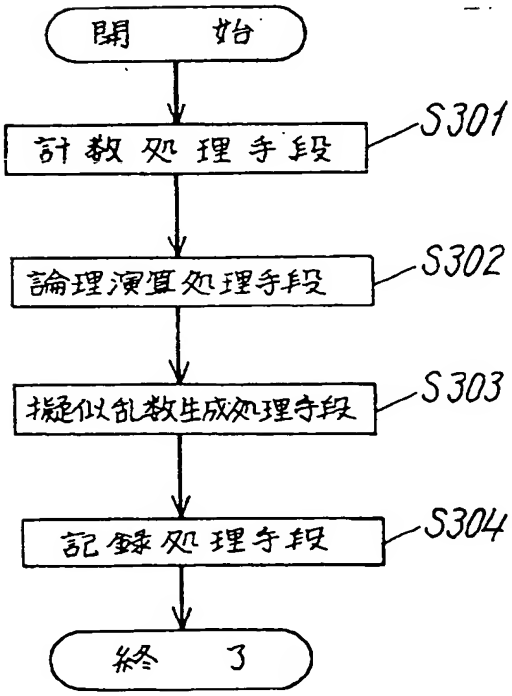
【図２】



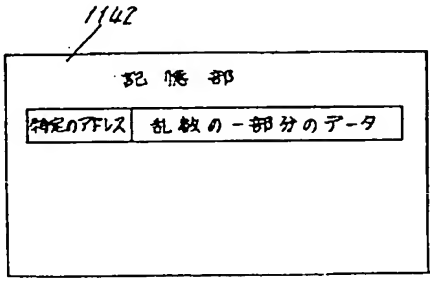
【図３】



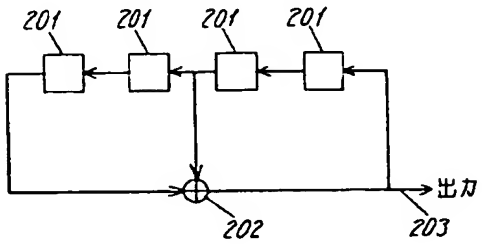
【図４】



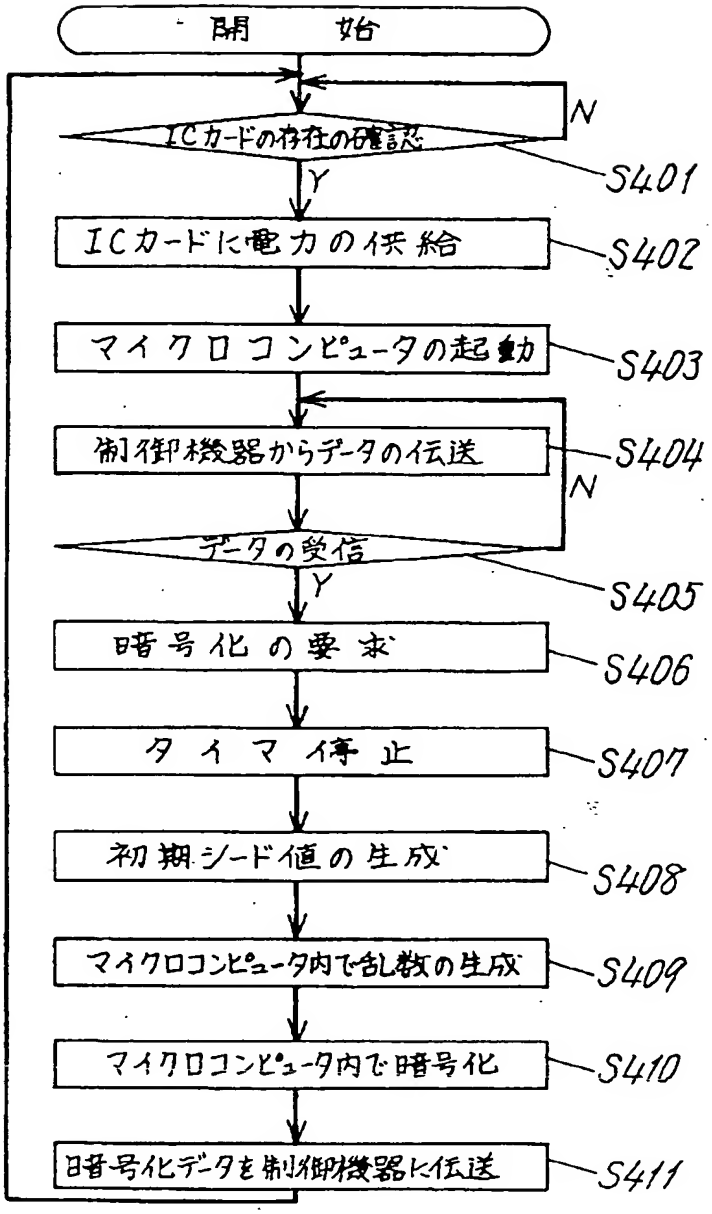
【図７】



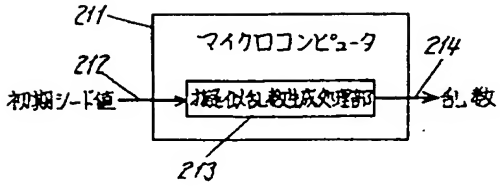
【図８】



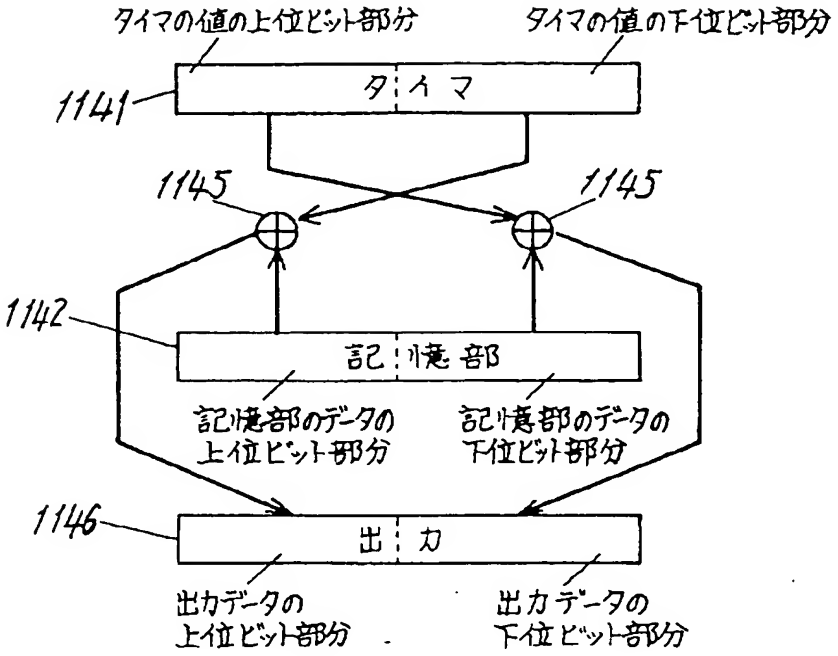
【図５】


開　始
ICカードの存在の確認
N
Y
S401
ICカードに電力の供給
S402
マイクロコンピュータの起動
S403
制御機器からデータの伝送
S404
N
データの受信
Y
S405
暗号化の要求
S406
タイマ停止
S407
初期シード値の生成
S408
マイクロコンピュータ内で乱数の生成
S409
マイクロコンピュータ内で暗号化
S410
暗号化データを制御機器に伝送
S411

【図９】


211
マイクロコンピュータ
214
212
初期シード値
擬似乱数生成処理部
乱数
213

【図6】


タイマの値の上位ビット部分
タイマの値の下位ビット部分
1141
タイマ
1145
1145
1142
記憶部
記憶部のデータの
上位ビット部分
記憶部のデータの
下位ビット部分
1146
出力
出力データの
上位ビット部分
出力データの
下位ビット部分